ASME Critical Assets Protection Initiative

ASME Homeland Security

ASME Risk Analysis and Management for Critical Assets Protection (RAMCAP) Methodology Document

PS&S Interagency Working Group

September 17, 2004

Dr. James W. Jones- Project Coordinator

RAMCAP Phase I Project Objectives

Produce technical basis document that describes overall methodology and provides a common framework for homeland security risk analysis decision-making

- **Common terminology**
- **Common metrics for comparing risks across sectors**
- **Common basis for reporting results**
- **Basis for informing resource allocation decisions**
  - **Countermeasures**
  - **Consequence mitigation actions**

RAMCAP Concept Development

The Executive Office of the President's Office of Science and Technology Policy (OSTP) sponsored a workshop on Critical Infrastructure Protection Priorities (CIPP) on September 23-24, 2002

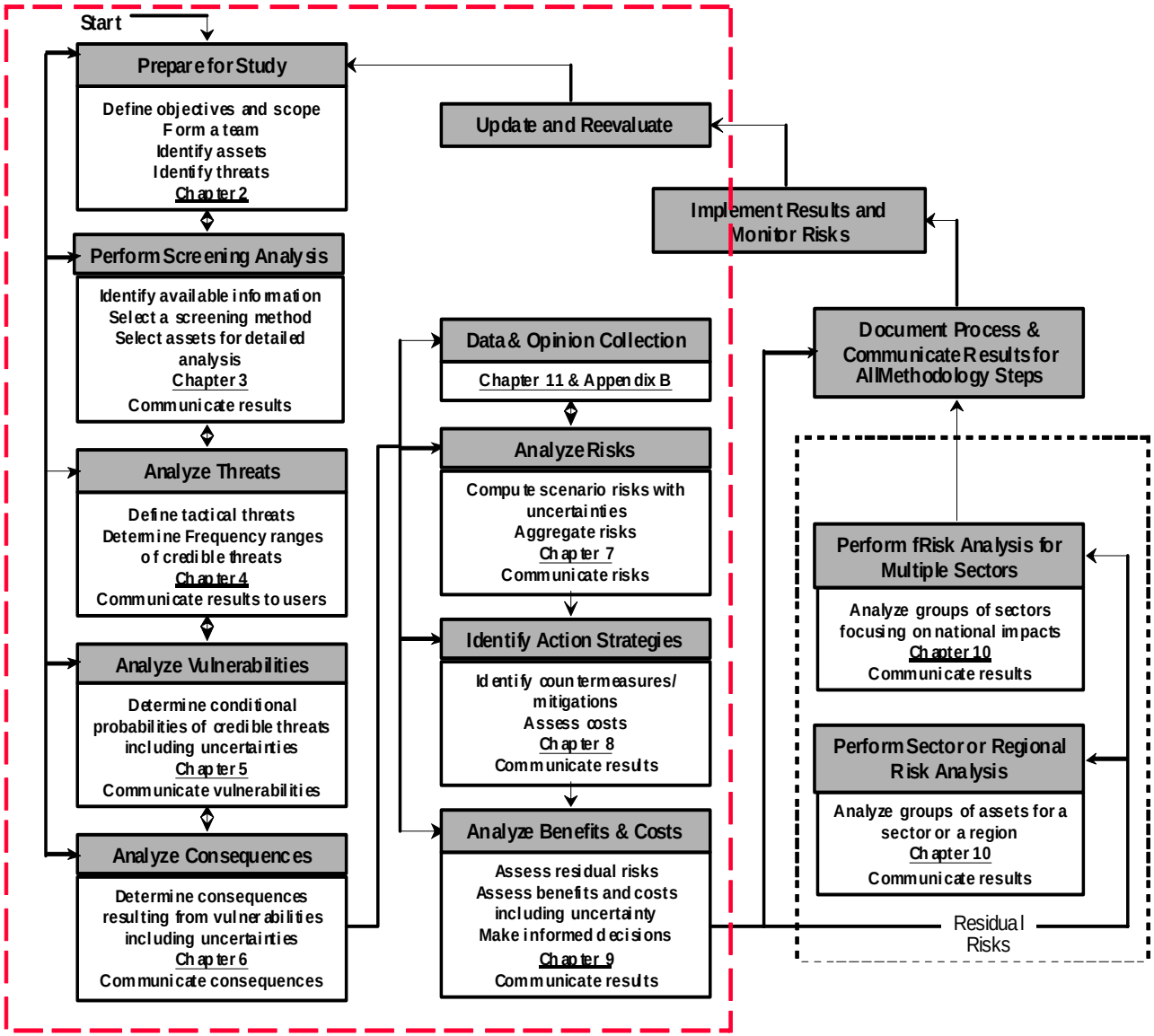
- **Over 90 industry leaders and government officials participated**
- **Topic: Role of Science and Technology in Countering Terrorism**
- **Key priorities were identified**
- **Guidance on the use of risk-based evaluation methods was identified as the top priority**
- **Risk-based methods are needed by both the private and the public sector for informing resource allocation decisions**
- **ASME awarded grant by the Department of Homeland Security to develop uniform risk-based guidance in September 2003**

RAMCAP Guidance Document Status

The RAMCAP methodology document is in the final stages of preparation for the Department of Homeland Security

- **Initial draft prepared in April 2004**
- **Workshop with some 125 interested parties held on April 14-16**
- **Numerous comments received from over 100 peer reviewers from industry, academia, and government**
- **Briefing with security professionals held on June 1-2, 2004**
- **Simplified version (Asset Application Handbook) prepared**
- **Both RAMCAP and Handbook under peer review**
- **Revision 0 to be delivered to DHS by early 2005**

Overall RAMCAP Methodology



Basic Risk Equation 1

$$R_{ai} = F_{ai} \times (Vulnerability)_{ij} \times (Consequences)_{ij}$$

Where:

R_{ai} = the annual economic risk for a given threat *i*

F_{ai} = the annual frequency of an adversary attacking a critical asset using a specific type of threat, *i*

Vulnerability = the conditional probability that a specific failure mode, *j*, will occur, assuming that the assumed threat, *i*, has occurred

Consequences = total measure of consequences of failure for threat *i* failing in mode *j*

Basic Risk Equation 2

$$R_{ijk} = F_{ai} P_{fij} P_{cijk} C_{cijk}$$

Where:

R_{ijk} = the economic risk

F_{ai} = the annual frequency of an adversary attacking a critical asset using a specific type of threat,

P_{cijk} = the combination of the probability ranges at each node of the event tree starting at the node, after the node where P_{fij} is defined,

P_{fij} = conditional probability of failure mode ***j*** due to threat **i**

Frequency of Occurrence

F_{ai} = the annual frequency of an adversary attacking a critical asset using a specific type of threat, *i*

If F_{ai} is set to 1.0, then the calculated risk is termed ***"Conditional-threat risk"***

Conditional-threat risk can be used to evaluate alternatives and to calculate the probability of occurrence that will justify the cost of countermeasures or mitigation strategies. Conditional risk cannot be used to calculate for comparison across diverse assets or sectors.

Vulnerability

- The vulnerability of an asset can be changed by employing countermeasures that will reduce the probability that a particular attack scenario will be successful.

- An example of a countermeasure is hardening the asset to explosives.

Consequences

- The consequences of failure for a particular attack scenario can be reduced by employing mitigation strategies.

- An example of a mitigation strategy is to insure early detection of a chemical or biological release.

Risk Management

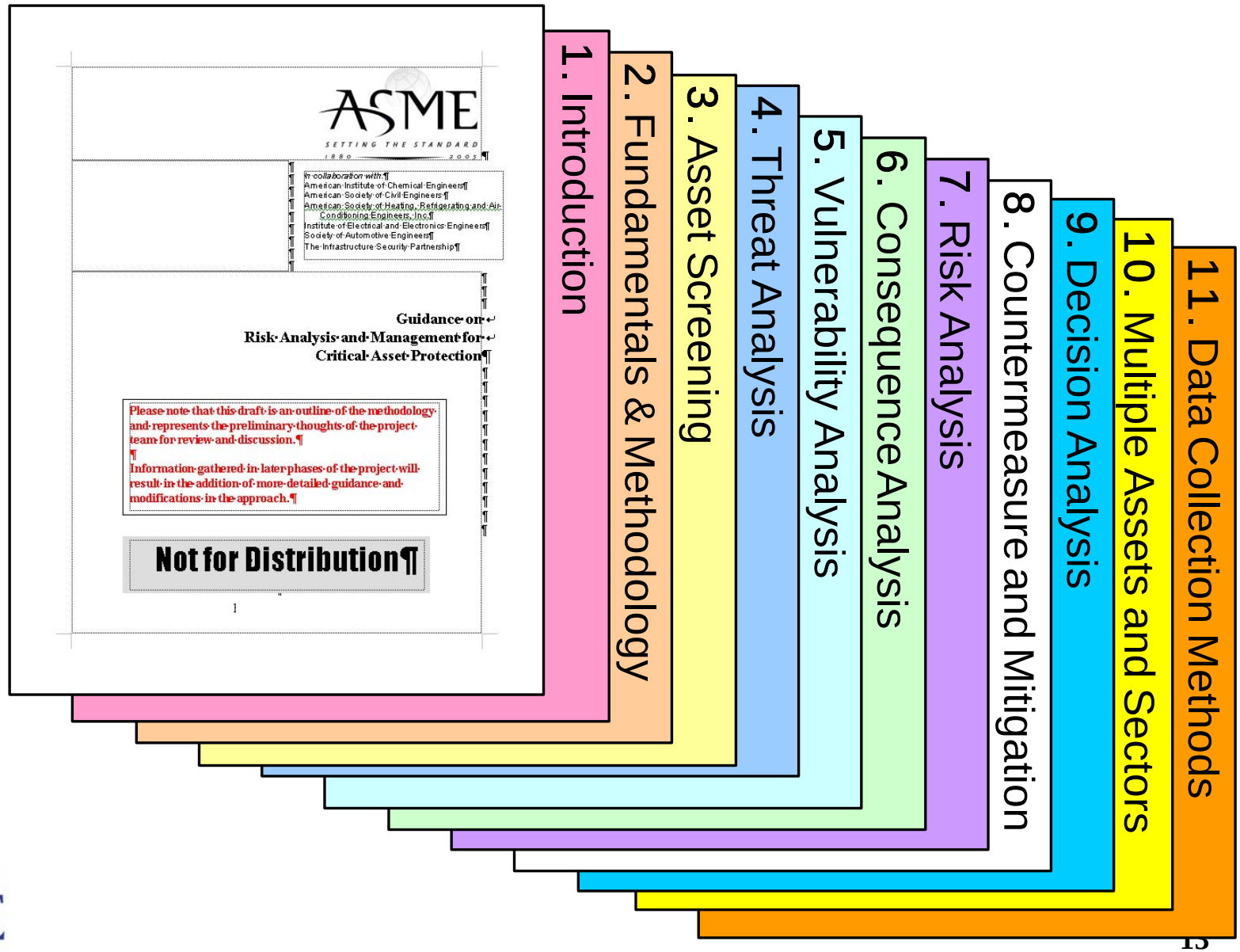
- Risk management is the process of determining the most beneficial combination of countermeasures and mitigation strategies that can be employed within the constraints the available resources.

- The risk equation can be used to evaluate alternatives and to select the best available practices. Conditional risk methods can be used to compare like assets. A complete risk analysis is necessary to compare risk across diverse assets and sectors.

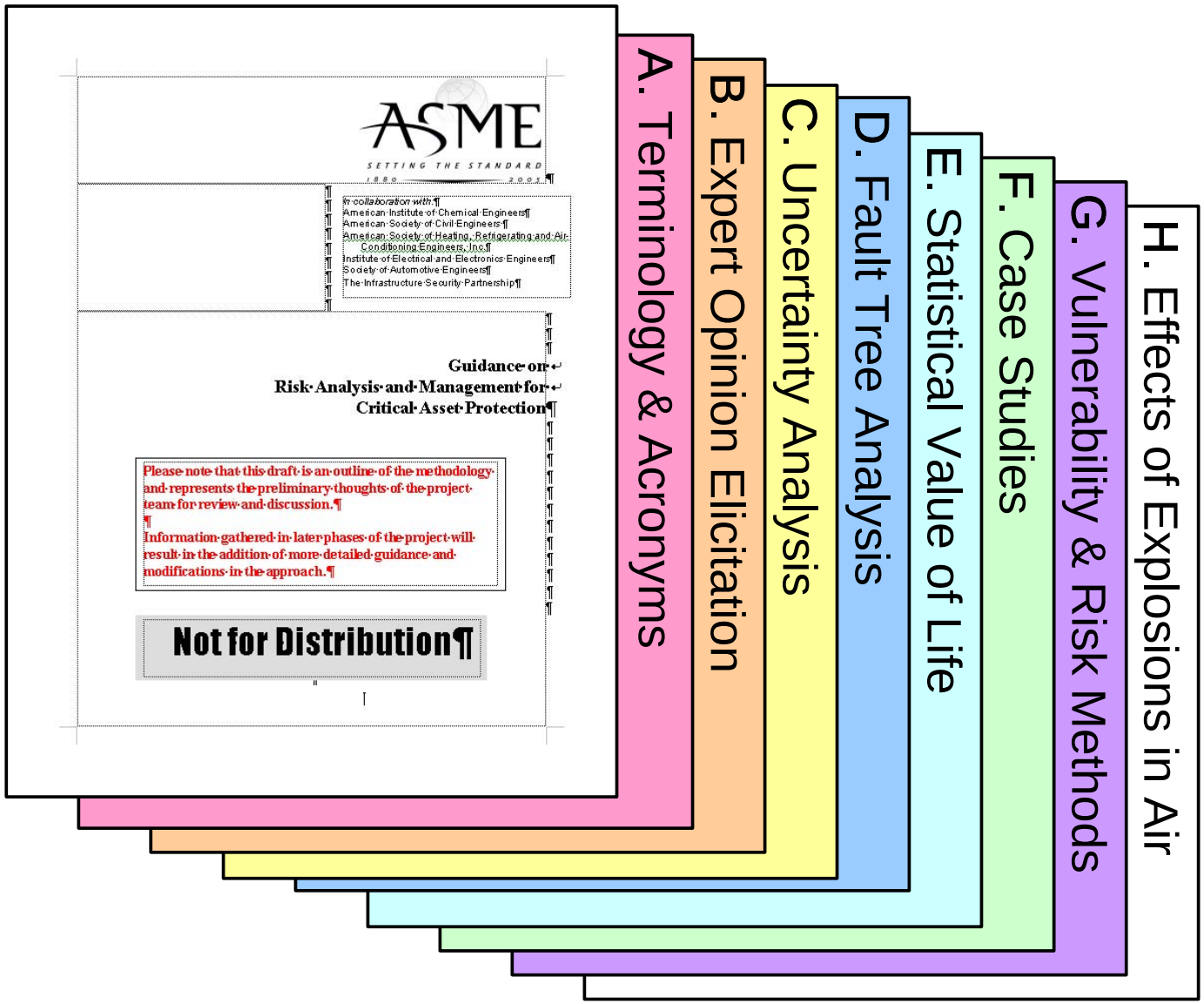
RAMCAP Document Description

- Current document is a reference document rather than a guidance document
- Provides technical basis for Asset Application Handbook (individual asset screening)
- Provides technical basis for Phase II sector-specific vulnerability assessment guidance
- Administrative guidance (e.g. roles and responsibilities) is not in scope
- Background and explanatory information included

RAMCAP Document Outline



RAMCAP Document Outline



RAMCAP Document Outline

Chapters 1 - 4 provide:

- Introduction
- Terminology (also see Appendix A) and overview of the methodology
- Screening methods – can be used as stand alone guidance or supplemented by the Asset Application Handbook
- Threat analysis – a threat frequency approach is recommended for higher levels of decision-making (national or regional), but is not needed at the asset level

RAMCAP Document Outline

Chapters 5 - 10 cover the sequential steps in the application of the methodology:

- Vulnerability analysis
- Consequence analysis
- Risk analysis
- Countermeasures and mitigation
- Decision analysis
- Multiple assets and sectors

Chapter 11 covers data collection methods

RAMCAP Document Description

- Qualitative screening (see Asset Application Handbook) to screen out assets or identify critical assets for further analysis
  - Primary screening at the asset owner level
  - Risk rating categories “calibrated” for consistency
- The absence of threat information leads to semi-quantified risk calculations (conditional-threat risk) and conditional-threat risk thresholds to support decision-making
- Risk ratings from 0 to 5 or from 0 to 10, based on existing methods and completed qualitative assessments, can be quantified and used to evaluate countermeasures and mitigation measures
- If threat information can be quantified, full Quantitative Risk Assessment (QRA) is possible

Phase II Project Scope

- Use RAMCAP document as overall reference
- Integrate key features of RAMCAP document that cover Security Vulnerability Assessment (i.e., threat and consequence analyses) into existing sector-specific methods, metrics, and documentation
- Assist sector organizations in developing new Security Vulnerability Assessment methods, metrics, and documentation, as appropriate

Phase II Project Scope

Applicable to 9 critical asset sectors:

- Commercial nuclear power plants
- Commercial nuclear spent fuel storage facilities
- Chemical plants
- Petroleum refineries
- Liquefied Natural Gas (LNG) storage facilities
- Subway Systems (including bridges and tunnels)
- Railroad Systems (including bridges and tunnels)
- Highway Systems (including bridges and tunnels)
- Power generation and transmission facilities

Phase II Project Scope

Two of the nine sectors are “pilot” sectors:

- The guidance for commercial nuclear power plants will build on the RAMCAP document and on existing vulnerability assessment guidance prepared by EPRI for the U. S. commercial nuclear power industry and vetted by the Nuclear Energy Institute (NEI)
- The sector-specific guidance for chemical plants will build on the RAMCAP document and existing guidance prepared by the American Chemistry Council and the American Institute of Chemical Engineers (AIChE)

Closing Commentary

- Risk-informed decision making has been used successfully by industry and government for many years.
- Cost-benefit analysis is an important tool to prioritize the allocation of national resources in the war on terrorism.
- Quantified measures are needed for benefit-cost analysis.
- Even if risk can be quantified only within very broad ranges, the results provide a much better basis for informing decisions than the use of judgment alone.